КІБЕРБЕЗПЕКА: освіта, наука, техніка

CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE

№4 (8), 2020

ISSN 2663 - 4023

DOI: 10.28925/2663-4023.2020.8.8596

УДК 004.056.2:378.147

Жданова Юлія Дмитрівна
канд. ф.-м. наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Спасітєлєва Світлана Олексіївна
канд. ф.-м. наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0003-4993-6355
s.spasitielieva@kubg.edu.ua,

Шевченко Світлана Миколаївна
канд. пед. наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Кравчук Катерина Володимирівна
студентка Факультету інформаціонних технологій та управління
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID: 0000-0002-3589-8784
kvkravchuk.fitu16@kubg.edu.ua

ПРИКЛАДНІ ТА МЕТОДИЧНІ АСПЕКТИ ЗАСТОСУВАННЯ ХЕШ-ФУНКЦІЙ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Анотація. В статті розглянуто застосування алгоритмів хешування в інформаційній безпеці з точки зору їх поступового та різнобічного вивченні в дисциплінах підготовки фахівців спеціальності 125 Кібербезпека у Київському університеті імені Бориса Грінченка. Проаналізовані сучасні алгоритми хешування, які є дуже затребуваними в сучасних цифрових технологіях, зокрема, в задачах забезпечення інформаційної безпеки сучасних інформаційно-комунікаційних систем. Виявлена і обґрунтована необхідність пильного вивчення хешування як окремого засобу забезпечення інформаційної безпеки. У публікації наведено ретельний і детальний аналіз типових завдань захисту з участю алгоритмів хешування таких, як реалізація структур для ефективного збереження великих масивів даних; пошук і зберігання даних в базах даних; захист паролю в процесі автентифікації; формування електронного цифрового підпису; контроль цілісності і достовірності важливих файлів, так і новітніх цифрових технологій блокчейну і створення криптовалют. Зроблено огляд та порівняння спеціальних програм для розрахунку хеш-кодів файлу або тексту, які пропонуються у вигляді додатків та онлайн сервісів. Серед засобів, що застосовуються для опанування студентами практичних навичок хешування зроблено наголос на використовуванні криптографічних служб CryptoAPI, Cryptography Next Generation і Security.Cryptography .NET Framework. Розглядаються базові криптографічні функції, що реалізують алгоритми хешування. Визначено перспективні напрями дослідження хешування для впровадження в навчальний процес, а саме: нечітке хешування, квантове хешування. З проведеного дослідження зроблено висновок про необхідність теоретичного і практичного вивчення хешування протягом всього терміну підготовки майбутнього спеціаліста з інформаційної безпеки.

Ключові слова: захист інформації; хеш-функція; хешування; алгоритми хешування; криптографічні сервіси.

ISSN 2663 - 4023

1. ВСТУП

Постановка проблеми. В сучасних умовах інформатизації суспільства, коли впроваджується велика кількість автоматизованих та інформаційно-управляючих систем в різних областях людської діяльності, перехід до нових технологій приводить не тільки до можливостей, яких не було раніше, але й до виникнення проблем, яких не було раніше. В зв'язку з цим зростає значущість проблеми забезпечення безпеки та захисту інформації, що циркулює, зберігається і оброблюється в таких системах, причому ця проблема стає все більш важливою з розвитком інформаційних систем з віддаленим доступом до спільних ресурсів, територіально розподілених систем, багатофункціональних інформаційних центрів тощо.

Впровадження глобальних комунікацій в ділове і повсякденне життя привело до розвитку систем електронного обміну даними, користувачами яких можуть бути державні, комерційні і некомерційні установи, а також окремі громадяни. З розповсюдженням таких систем не тільки автоматизується і прискорюється створення, обробка електронних документів, а й значно підвищується їх уразливість. В таких системах задача забезпечення цілісності електронних документів виходить на перше місце.

Доступність персональних обчислювальних засобів і пристроїв у вигляді персональних комп'ютерів і смартфонів, розповсюдження спеціальних знань і навичок користування такими засобами і пристроями серед населення привели не тільки до значного полегшення виконання розумових задач, але й до значного збільшення загроз інформаційно-комунікаційним системам у вигляді спроб несанкціонованого доступу до них. При цьому спостерігається збільшення числа глобальних витоків конфіденційної інформації майже в 3 рази у порівнянні з минулим роком [1].

При вирішенні зазначених вище проблем забезпечення інформаційної безпеки сучасних інформаційно-комунікаційних систем важливе місце посідають наступні завдання, які потребують

1) обробки дуже великої кількості даних різного формату (наприклад, при управлінні інцидентами інформаційної безпеки, при виявленні злоякісного програмного забезпечення);
2) виявлення однакових інформаційних об'єктів (наприклад, при перевірці достовірності).

Обидва зазначені типи завдань з успіхом вирішуються за допомогою спеціальних алгоритмів стиснення та швидкої обробки даних за допомогою хешування – перетворення за детермінованим алгоритмом масиву двійкових вхідних даних довільної довжини в двійковий рядок вихідних даних фіксованої довжини.

Всеохоплююче розповсюдження інформаційних технологій та разом з цим зростання проблем забезпечення інформаційної безпеки сучасних інформаційно-комунікаційних систем вимагають наявності спеціалістів, які можуть кваліфіковано і якісно вирішувати такі проблеми. Поява все нових і нових інформаційних технологій, постійний розвиток професійних компетенцій, запити роботодавців до знань та навичок спеціалістів з інформаційної безпеки вимагають постійно осучаснювати підходи до навчання таких спеціалістів, зокрема до формування практичних навичок, серед яких важливе місце посідає вміння правильно підібрати й застосувати алгоритм хешування, в залежності від конкретного завдання із забезпечення інформаційної безпеки сучасних інформаційно-комунікаційних систем. Формуванню саме практичних навичок приділяється велика увага на кафедрі інформаційної та кібернетичної безпеки

Київського університету імені Бориса Грінченка, яке здійснюється в межах компетентнісного підходу до навчання.

Аналіз останніх досліджень і публікацій. Термін «хешування» (hashing) в сучасному значенні з'явився порівняно недавно [2] в друкованих роботах з програмування, хоча сама конструкція була відома раніше. В перекладі з англійської іменник «*hash*» має декілька значень: «дрібно порублені овочі, мішанина, плутанина», а дієслово «*hash*» означає «рубати, кришити, перемішувати». Огляди із застосування хешування в програмуванні можна знайти, наприклад, в [3]. Застосування хешування у задачах забезпечення захисту інформації розглянуто в [4].

Значення хешування для захисту інформації важко переоцінити. Сьогодні хеш-аналіз використовують як для типових завдань захисту, а саме:

- пошук і зберігання даних в базах даних;
- захист паролю в процесі автентифікації;
- формування стисненого образу при створенні електронного цифрового підпису;
- контроль цілісності і достовірності важливих файлів,

так і для сучасних технологій блокчейну і створення криптовалют, де хеш забезпечує цілісність ланцюжка транзакцій [5].

Формування здатності майбутніх спеціалістів з інформаційної безпеки адекватно реалізовувати свої знання в конкретних ситуаціях здійснюється на кафедрі інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка згідно Освітній програмі [6] і визначається існуючою моделлю розвитку професійних компетенцій [7]. Прийнята концепція компетентнісного підходу корелює очікувані результати освітньої діяльності з міжпредметними зв'язками [8].

Мета статті. Метою даної статті є огляд та аналіз існуючих підходів до використання хешування для захисту інформації та висвітлення особливостей методики формування практичних навичок з вирішення задач інформаційної безпеки методом хешування у студентів в процесі вивчення дисциплін підготовки фахівців спеціальності 125 Кібербезпека.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Хеш-функція H – функція, що здійснює алгоритм хешування – є ін'єкцією з множини M масивів двійкових вхідних даних m довільної довжини в двійковий рядок $h = H(m)$ вихідних даних фіксованої (звичайно невеликої) довжини. Хеш-функцію також ще називають функцією згортки, вхідний масив M називають прообразом, вихідний рядок $H(m)$ – хеш-образом, хеш-кодом, цифровим відбитком, дайджестом, або просто хешем.

Хеш-функція має задовольняти вимоги:

1) Для будь-якого $m \in M$ легко обчислити $h = H(m)$.

2) Для будь-якого h важко обчислити m таке, що $h = H(m)$.

В зв'язку з тим, що алгоритм хешування напрямлений перш за все на максимальне стиснення вхідних даних, можливі колізії, тобто поява однакових хеш-образів в різних прообразів. Тому хеш-функція має задовольняти ще вимогу

3) Для будь-якого $m \in M$ важко знайти $m' \in M$ таке, що $h = H(m) = H(m')$.

ISSN 2663 - 4023

Умови 1)-3) вказують на однонапрямленість хеш-функції. Крім однонапрямленості, часто висувають ще вимогу:

4) Важко знайти $m,m' \in M$ такі, що $h = H(m) = H(m')$.

В залежності від типу завдання, яке потрібно вирішити за допомогою хешування для забезпечення інформаційної безпеки сучасних інформаційно-комунікаційних систем всі алгоритми хешування умовно поділяються на два великі класи:

1) ті, які швидко обчислюються: їх застосовують для обробки великої кількості даних різного формату.

2) ті, які мінімізують число колізій: їх застосовують для обробки малої кількості даних з метою виявлення однаковості інформації.

Існує виділений клас хеш-функцій – криптографічні, до яких висуваються більш жорсткі вимоги, наприклад, до довжини хеш-коду, до загальнодоступності алгоритму хешування.

В залежності від специфіки задачі, що розв'язується, хеш-функції, що здійснюють алгоритми хешування, розрізняють за параметрами:

- швидкість обчислення;
- ймовірність утворення колізії;
- існування лавинового ефекту.

Сьогодні існує велика кількість алгоритмів хешування з різними параметрами, серед яких найбільше розповсюдження отримали наступні:

- алгоритми CRC16/32 (Cyclic Redundancy Check – циклічна перевірка надлишків) – контрольна сума (перетворення не є криптографічним), потужний легко обчислюваний метод захисту інформації з високим рівнем виявлення помилок та простотою застосування. Найбільш популярний CRC32, який формує хеш розміром 32 біти.
- алгоритми MD2/4/5/6 (Message Digest) – криптографічні, серед яких найбільшу популярність знайшов MD5 з розміром хешу 128 бітів, який застосовується для зберігання паролів, для створення криптографічних ключів, для формування електронного цифрового підпису. До недоліків цього алгоритму відноситься висока ймовірність колізій.
- алгоритми сімейства SHA (Secure Hash Algorithm), – криптографічні, серед яких SHA-1 з розміром хешу 160 бітів є стандартизованою хеш-функцією для застосування в держструктурах США, але зараз йде перехід до більш сильної версії SHA-2, яка містить алгоритми SHA224, SHA256, SHA384 і SHA512, причому SHA224 і SHA384 є аналогами SHA256 і SHA512 відповідно, де частина хеш-коду відкидається після обчислення. Алгоритм SHA256 рекомендований для застосувань в умовах вимог підвищеної безпеки.
- алгоритм ГОСТ Р 34.11-2012 «Стрибог» – стандарт РФ, складається з пари хеш-функцій з розміром хешу 256 і 512 бітів, які відрізняються початковим станом і результатом обчислень. Має високу криптостійкість та швидкість роботи.
- алгоритм ДСТУ 7564:2014 «Купина» – стандарт України, функція стиснення складається з двох фіксованих 2n-бітних перестановок, що повторюють такі самі перестановки шифру «Калина»; розмір хешу від 8 до 512 біт.

До того ж, має місце метод універсального хешування, коли вибір хеш-функції здійснюється випадково із заданої множини. Використання універсального хешування гарантує низький рівень колізій. Універсальне хешування знайшло застосування в реалізації хеш-таблиць і криптографії [9].

ISSN 2663 - 4023

Останнім часом набуло перспективного розвитку нечітке хешування [10], яке, зокрема, дозволяє вирішити проблему пошуку подібних, але не тотожних інформаційних об'єктів, що є актуальною, наприклад, при виявленні злоякісних програмних продуктів.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Хешування як алгоритм, що оперує короткими значеннями, дуже затребуване в цифрових технологіях, які вимогливі до об'єму вхідних даних, адже значно простіше опрацьовувати малооб'ємні однотипні файли, ніж документи великого об'єму і різного формату. Крім того, на сьогоднішній день фактично жоден прикладний криптографічний засіб не може обійтися без застосування хешування. Хешування заслуговує пильного вивчення як окремий засіб забезпечення інформаційної безпеки.

Розглянемо основні застосування хеш-функцій в інформаційній безпеці та методи формування практичних навичок застосовування хешування при вивченні дисциплін підготовки студентів спеціальності 125 Кібербезпека.

Створення ефективної інформаційної структури. За допомогою хешування інформація структурується у вигляді хеш-таблиць, побудова яких дозволяє здійснювати швидкий пошук, додавання або видалення потрібних відомостей, причому всі три операції виконуються за середній час $O(1)$ [11]. Хеш-таблиці є структурою для ефективного збереження великих розріджених масивів даних. В мовах об'єктно-орієнтованого програмування (C++, C#, Java) реалізовані класи для роботи з колекціями об'єктів, які зберігаються в хеш-таблицях. Інформація про об'єкти будь якої складності зберігається в хеш-таблицях за допомогою механізму хешування. При хешуванні визначається унікальний хеш-код з використанням інформаційного вмісту спеціального ключа. Хеш-код використовується як індекс, за яким в таблиці зберігаються дані, які відповідають заданому ключу. Такий самий принцип використовується при пошуку даних за індексом у SQL базах даних.

В сучасних NoSQL базах даних типу «ключ-значення» (Redis, BigTable, Memcached) широко використовується хешування [12]. Хеш-таблиця є однією із п'яти структур збереження даних в моделях ключ-значення. Також хешування використовується для операцій з даними, що забезпечує сталий час виконання операцій пошуку, вилучення та додавання значень незалежно від величини масивів даних.

Всебічний огляд використання та практичні навички реалізації хеш-таблиць студенти отримують в рамках вивчення дисциплін «Технології безпечного програмування» та «Захист баз та сховищ даних».

Узагальненням методу звичайних хеш-таблиць є геометричне хешування – метод для розв'язування задач на площині або в тривимірному просторі, який використовується в комп'ютерній графіці для пошуку найближчих пар в множині точок або для пошуку однакових зображень. Елементи хеш-таблиці (яка в цьому випадку називається файл сітки) мають не менше двох індексів. Геометричне хешування також застосовується в телекомунікаціях при роботі з багатовимірними сигналами.

Захист паролів. Хешування є ідеальним способом зберігання паролів, адже більшість серверів зберігає паролі користувачів у вигляді їх хешів. Доступ до ресурсу здійснюється порівнянням хеш-коду паролю, що вводиться користувачем, з хеш-кодом, що зберігається на сервері.

ISSN 2663 - 4023

Ця область застосування хешування знайома кожному користувачу. Студенти спеціальності 125 Кібербезпека починають формувати практичні навички хешування для захисту паролів починаючи із дисципліни «Вступ до спеціальності», і продовжуючи в інших, що формують фахові компетенції, зокрема «Основи інформаційної і кібербезпеки та захисту інформації», «Захист інформації в інформаційно-комунікаційних системах», «Основи захисту конфіденційних даних». На практичних і лабораторних заняттях студенти мають можливість моделювати парольний захист із застосуванням криптографічних хеш-функцій. Майбутні спеціалісти із захисту інформації мають свідомо ставитися до вимог сучасних онлайн-сервісів до паролів: довжина паролю має бути не менше 6 символів; пароль має містити цифри і букви в різних регістрах. Чим складніше буде пароль, тим менше ймовірність його злому, адже для простих паролів існують бази даних відповідностей паролів та їх хеш-кодів, якими широко користуються зловмисники. Існують безліч атак, що дозволяють відновити паролі з простих хеш-кодів, і одне із завдань вищезгаданих дисциплін є навчити студентів знижувати ефективність цих атак.

Створення електронного цифрового підпису. Хеш-функція називається криптостійкою, якщо вона стійка до відновлення початкових даних за хеш-кодом, і стійка до колізій. Насправді, відновлення початкових даних за хеш-кодом можливе завжди, тільки час відновлення такий, що практично не реалізується. Будь-яка криптостійка хеш-функція є криптографічною і може бути застосована для контролю цілісності даних, що передаються, який здійснюється за допомогою електронного цифрового підпису – невеликої додаткової цифрової інформації, побудованої за початковим повідомленням. Електронний цифровий підпис створюється за допомогою асиметричних алгоритмів шифрування і алгоритмів хешування і супроводжує документ, що пересилається. Якщо в ході порівняння хеш-коди двох інформаційних наборів виявляються однаковими, то документ, що пересилається, визнається дійсним, а підпис вірним. Методика використання електронного цифрового підпису описана в сучасній літературі з криптографії, наприклад, в [13].

Студенти спеціальності 125 Кібербезпека мають можливість досконало оволодіти методами побудови електронного цифрового підпису з використанням різних схем асиметричного шифрування під час виконання практичних завдань з дисципліни «Прикладна криптологія». Із застосуванням технології електронного цифрового підпису для реалізації таких процесів інформаційного захисту як автентифікація об’єкта або суб’єкта інформаційної мережі студенти знайомляться під час вивчення дисциплін «Стандарти інформаційної та кібербезпеки», «Криптомеханізми інформаційної та кібербезпеки», «Інфраструктура відкритих ключів». Практична навчальна діяльність студентів відбувається за індивідуальними завданнями.

Забезпечення цілісності і підтвердження авторства інформації, що передається, гарантується імітовставкою або MAC-кодом (Message Authentication Code), що є нічим іншим, як хеш-кодом повідомлення, схема утворення якого використовує симетричне шифрування, наприклад, DES в режимі CBC, або ДСТУ ГОСТ 28147:2009 в режимі вироблення імітовставки. Імітовставки на основі хеш-функцій HMAC (Hash-based MAC) також використовуються в криптографічному протоколі TLS, що забезпечує захищену передачу даних між вузлами в мережі Інтернет. З цим питанням студенти знайомляться під час вивчення дисциплін «Прикладна криптологія», «Захист інформації в інформаційно-комунікаційних системах», «Технології безпеки мережевої інфраструктури».

ISSN 2663 - 4023

Контроль цілісності і достовірності важливих файлів здійснюється за допомогою алгоритмів хешування. Так, хеші файлів, розташовані на сайтах розробників, дозволяють переконатися в їх цілісності при завантаженні з альтернативних джерел мережі Internet. Програми, що використовуються для пошуку на комп'ютері файлів-дублікатів, працюють, як правило з хеш-образами таких файлів. Крім того, перевірка хешів системних файлів дозволяє виявити наявність злоякісного програмного забезпечення. Про такі і багато інших варіантів застосування хешування для контролю цілісності і достовірності студенти спеціальності 125 Кібербезпека дізнаються під час вивчення дисциплін «Захист інформації в інформаційно-комунікаційних системах», «Основи ОС та сучасних Інтернет-технологій».

Спеціальні програми для розрахунку хеш-кодів. Під час виконання практичних завдань, які потребують обчислення хеш-кодів, студенти можуть виконувати розрахунки як вручну, якщо завдання має на меті допоміжне використання хеш-функцій, так і за допомогою спеціальних програм. Сьогодні можна знайти багато прикладних програм для розрахунку хеш-коду файлу або тексту як онлайн, наприклад, Convert String [14], FoxTools, та безліч їм подібних, так і безпосередньо на комп'ютері, наприклад, HashTab, Hash Calculator, Hash Tool та інші. Серед останніх привертає увагу утиліта HashTab (Рис.1.). Вона є розширенням провідника Windows, вбудовується у вигляді вкладки у властивості файлу і є безкоштовною для приватного використання. Крім того, програма HashTab може працювати і в Mac OS.

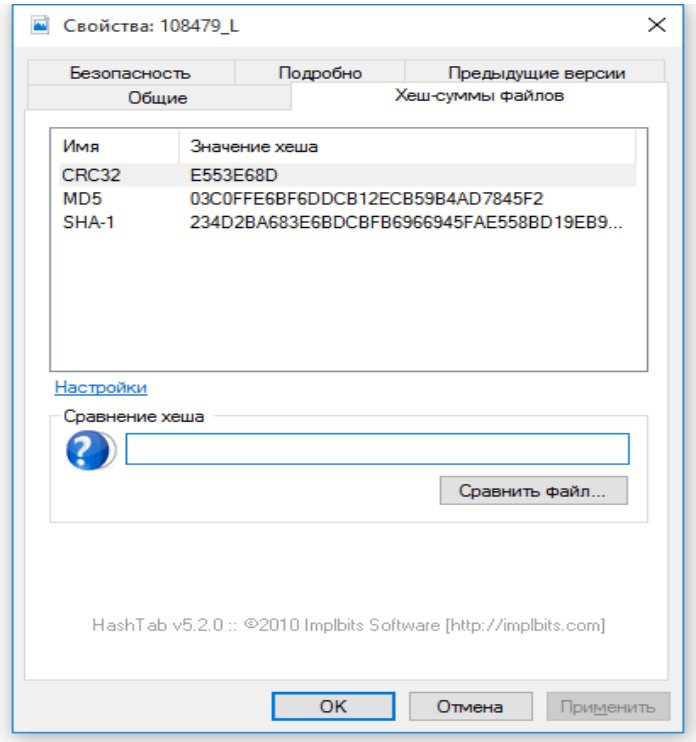

Рис.1. Вікно властивостей файлу із вбудованою вкладкою HashTab

Хешування із застосуванням криптографічних служб CryptoAPI і .NET. Криптографічні служби різного призначення як прикладного рівня, так і рівня ядра є підсистемами сучасних операційних систем Microsoft. Найвідомішою серед них є Crypto API (Cryptography API, CAPI), Cryptography Next Generation (CNG),

Security.Cryptography .NET Framework [15]. Серед завдань, які вирішуються за допомогою криптографічних служб, відзначимо шифрування даних з можливістю їх подальшої передачі; перевірку достовірності та цілісності інформації, роботу з визнаними криптографічними стандартами. Одна з основних функціональних груп криптографічних служб – базові криптографічні функції – містить функції, що реалізують алгоритми хешування.

Категорія алгоритмів реалізується на основі розширюваного шаблону (шаблону), включаючи два рівня наслідування. На рис. 2 представлено ієрархію класів для алгоритмів хешування. На вершині ієрархії розміщений абстрактний базовий клас, ім'я якого відповідає типовому алгоритму – HashAlgorithm. Від базового абстрактного класу успадковується абстрактний клас другого рівня, який забезпечує відкритий інтерфейс для використання даного алгоритму. Реалізація алгоритму є похідною від класу другого рівня; саме її екземпляр створює і використовує клієнтський додаток. Криптографічні бібліотеки надають багато керованих реалізацій алгоритмів, а також класи – "обгортки" для вбудованих реалізацій з CryptoAPI та CNG.

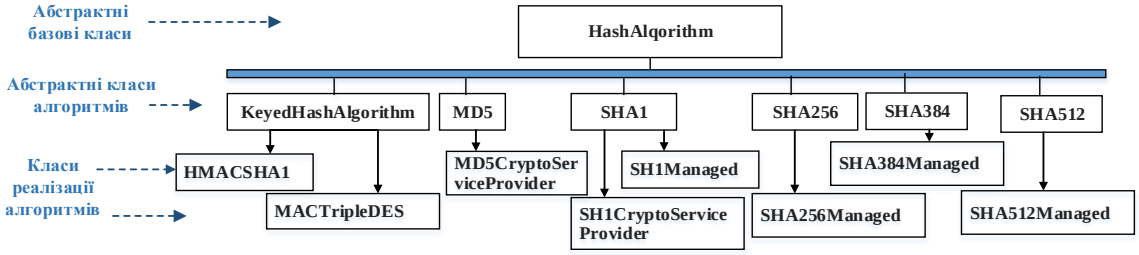

Рис.2. Класи хеш-алгоритмів Security.Cryptography .NET

Реалізовані алгоритми криптографічних служб можна використовувати для програм створення системи автентифікації, захищеної електронної пошти, забезпечення конфіденційність даних тощо. Студенти мають використовувати наведені хеш-алгоритми для забезпечення цілісності оброблювальних даних при вивченні дисципліни «Технології безпечного програмування».

Використання в блокчейнах і в криптовалютах можна відзначити серед інших застосувань хешування. Саме хешування за допомогою криптографічної хеш-функції дає можливість здійснювати операції обміну криптовалют і надійний захист блокчейнів. Структура даних блокчейн – це упорядкований «назад» пов'язаний між собою список блоків транзакцій (рис.3). Кожен блок у блокчейн ідентифікується хешем, який генерується з використанням криптографічного алгоритму SHA256, застосованого до заголовка блоку [16]. Кожен блок також містить хеш свого батька всередині власного заголовка.

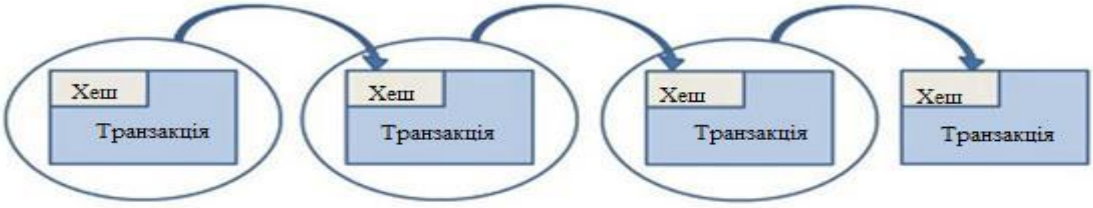

Рис. 3. Ланцюг блоків транзакцій з використанням хешів

Послідовність хешів, що зв'язують кожен блок з його батьком утворює ланцюг, який тягнеться до самого першого блоку, відомому як блок генезису. Змінений хеш батьківського блоку вимагає зміни посилання "хешу попереднього блоку" в дочірньому блоці. Це каскадний ефект гарантує, що якщо блок має багато поколінь, він не може бути змінений без перегляду всіх попередніх блоків. Ті блоки, які вже записані в блокчейн, змінити неможливо. Криптографічні алгоритми хешування гарантують, що будь-яка зміна вхідних даних транзакції, навіть сама незначна, призведе до появи іншого значення хешу в результатах розрахунків, що вказує на ймовірність компрометації вхідних даних транзакції. Так як для подібного перегляду потрібна величезна кількість обчислень, то довгий ланцюг блоків робить глибоку історію в блокчейні незмінною, що є ключем до безпеки цифрового ресурсу.

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

На прикладі навчання хешуванню та його різноманітним застосуванням до задач забезпечення захисту інформації показано величезне значення вироблення саме практичних навичок, які відповідають сучасним вимогам до рівня підготовки фахівців спеціальності 125 Кібербезпека з боку роботодавців.

Згідно концепції компетентнісного підходу міжпредметні зв’язки мають потужний вплив на очікувані результати освітньої діяльності, тому з огляду на проведене дослідження можна зробити висновок про те, що всебічне теоретичне і практичне вивчення хешування протягом всього терміну підготовки майбутнього спеціаліста з інформаційної безпеки робить важливий внесок в перетворення напрацьованих знань та навичок в професійні компетенції.

Для подальших досліджень може бути проголошено декілька напрямків застосування хешування, які можуть бути додані в начальні програми дисциплін і які можуть поглибити компетентність майбутніх спеціалістів із захисту інформації. Серед них нечітке хешування, квантове хешування, застосування для захисту мобільних додатків. Слід відмітити, що точкові дослідження в цьому напрямі проводяться учасниками наукового товариства студентів та викладачів кафедри.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Глобальное исследование утечек конфиденциальной информации в первом полугодии 2019 года. [Онлайн] Режим доступу: https://www.infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf?rel=1 [20 лют. 2020]

[2] H. Hellerman. *Digital Computer System Principles*. McGraw-Hill, 1967.

[3] Д.Э. Кнут. *Искусство программирования. Том 3. Сортировка и поиск*. 2-е изд. М: Вильямс, 2007.

[4] И.Д. Горбенко, И.А. Штанько, "Функции хеширования. Понятия, требования, классификация, свойства и применение", *Радиоэлектроника и информатика*. Вып. 1, с. 64-69, 1998.

[5] Лоран Лелу, Блокчейн от А до Я. Все о технологии десятилетия, Москва, Россия, Изд-во «Эксмо», 2018.

[6] *Освітньо-професійна програма. 125.00.01. Безпека інформаційних і комунікаційних систем першого (бакалаврського) рівня освіти.* Київський університет імені Б. Грінченка, 2018. [Онлайн] Режим доступу: http://kubg.edu.ua/images/stories/Departaments/vstupnikam/fitu/2018/2019_bak_op_kiber.pdf [15 берез. 2020]

[7] В.Л. Бурячок, В.М. Богуш, Ю.В. Борсуковський, П.М. Складанний, В.Ю. Борсуковська, "Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України", *Інформаційні технології і засоби навчання,* том 67, №5, с.277-289, 2018.

[8] Ю.Д. Жданова, С.О. Спасітєлєва, С.М. Шевченко, "Формування у студентів IT-спеціальностей компетентностей в області захисту інформації з використанням криптографічних служб .NET FRAMEWORK", *Фізико-математична освіта*, 1(19). с. 48-54, 2019.
[9] Г. Халимов, *Универсальное хеширование.* LAP LAMBERT Academic Publishing, 2014.
[10] К.А. Тюрин, "Нечёткое хэширование в задачах информационной безопасности", *Обзор. НЦПТИ*, 1(16), с. 40-53, 2019.
[11] Н. Вирт, *Алгоритмы и структуры данных*. М: Мир, 1989.
[12] П. Дж. Садаладж, М. Фаулер, *NoSQL: новая методология разработки нереляционных баз данных*. М: Вильямс, 2016.
[13] Б. Шнайер, *Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си*. М.:Триумф, 2002.
[14] Хеш-функції - Онлайн Генератори хеш - Convert String [Онлайн] Режим доступу: https://www.convertstring.com/uk/Hash [8 берез. 2020]
[15] Ю.Д. Жданова, С.О. Спасітєлєва, С.М. Шевченко, "Застосування бібліотеки класів Security.Cryptography для практичної підготовки спеціалістів з кібербезпеки", *Кібербезпека: освіта, наука, техніка*, 4(4), с. 44-53, 2019.
[16] С.О. Спасітєлєва, В.Л. Бурячок, "Перспективи розвитку додатків блокчейн в Україні", *Кібербезпека: освіта, наука, техніка*, 1(1), с. 35-48, 2018.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (8), 2020
ISSN 2663 - 4023

Yuliia D. Zhdanova
PhD, Associate Professor, Associate Professor of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Svitlana O. Spasiteleva
PhD, Associate Professor, Associate Professor of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0003-4993-6355
s.spasitielieva@kubg.edu.ua

Svitlana M. Shevchenko
PhD, Associate Professor, Associate Professor of the Department of Information and Cyber Security
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Kateryna V. Kravchuk
Student of the Faculty of Information Technology and Management
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-3589-8784
kvkravchuk.fitu16@kubg.edu.ua

APPLIED AND METHODICAL ASPECTS OF USING HASH FUNCTIONS FOR INFORMATION SECURITY

Abstract. The article deals with the use of hashing algorithms for information security in training students of the specialty "125 Cybersecurity" at the Kiev Boris Grinchenko University. The modern hashing algorithms that are widely used in modern digital technologies, in particular, in the tasks of ensuring information security of modern information and communication systems has been analyzes in the article. The need for a thorough study of hashing as a means of ensuring information security has been identified and substantiated. The paper has present a thorough and detailed analysis of typical security tasks involving hashing algorithms such as implementing structures to efficiently store large data sets; searching and storing data in databases; password protection in the authentication process; formation of electronic digital signature; control of integrity and authenticity of important files; digital blockchain technologies and creation of cryptocurrencies. The special programs offered in the form of applications and online services for calculating hash codes of a file or text have been reviewed and compared. Among the tools used to provide students with practical hashing skills are the use of CryptoAPI, Cryptography Next Generation, and Security.Cryptography .NET Framework cryptographic services. Basic cryptographic functions that implement hashing algorithms have been considered. Prospective directions of hashing research for introduction into the educational process have been defined, namely: fuzzy hashing, quantum hashing. The study concluded that the need for a theoretical and practical study of hashing throughout the training of information security professionals.

Keywords: information security; hash function; hashing; hashing algorithms; cryptographic services.

REFERENCES

[1] Global'noye issledovaniye utechek konfidentsial'noy informatsii v pervom polugodii 2019 goda. (2019) [Global study of confidential information leaks in the first half of 2019] [Online]. Available: https://www.infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf?rel=1. [Feb. 20, 2020]. (in Russian).
[2] H. Hellerman. *Digital Computer System Principles*. McGraw-Hill, 1967.

[3] D.E. Knut. *Iskusstvo programmirovaniya. Tom 3. Sortirovka i poisk.* [*The Art of Computer Programming Volume 3: Sorting and Searchin*] 2nd ed. M.: Williams, 2007.

[4] I.D. Gorbenko, I.A. Shtan'ko, "Funktsii kheshirovaniya. Ponyatiya, trebovaniya, klassifikatsiya, svoystva i primeneniye" ["Hashing Functions. Concepts, Requirements, Classification, Properties and Applications"], *Radioelectronics and Computer Science.* Vol. 1, p. 64-69, 1998. (in Russian).

[5] Loran Lelu, *Blokchein ot A do Ya. Vse o tekhnologii desyatiletiya. [Block from A to Z. All about the technology of the decade]*, Moskva, Rossiya, Izd-vo“Eksmo,”2018. (In Russian).

[6] *Osvitn'o-profesiyna prohrama. 125.00.01. Bezpeka informatsiynykh i komunikatsiynykh system pershoho (bakalavrs'koho) rivnya osvity.* Kyyivs′kyy universytet imeni B. Hrinchenka, 2018. [Educational and professional program. 125.00.01. Safety of information and communication systems of the first (bachelor) level of education. Kyiv Boris Grinchenko University, 2018] [Online] Available at: http://kubg.edu.ua/images/stories/Departaments/vstupnikam/fitu/2018/2019_bak_op_kiber.pdf [Mar. 15, 2020] (in Ukrainian).

[7] V.L Buryachok, V.M. Bohush, YU.V. Borsukovs′kyy, P.M. Skladannyy and V.YU. Borsukovs′ka, "Model′ pidhotovky fakhivtsiv u sferi informatsiynoyi ta kibernetychnoyi bezpeky v zakladakh vyshchoyi osvity Ukrayiny" ["Model of training specialists in the field of information and cybernetic security in higher education institutions of Ukraine"], *Information technology and Learning Tools*, 67(5), 277-289, 2018. (in Ukrainian).

[8] Yu.D. Zhdanova, S. Spasiteleva, S. and S.M. Shevchenko. "Formuvannya u studentiv IT-spetsial′nostey kompetentnostey v oblasti zakhystu informatsiyi z vykorystannyam kryptohrafichnykh sluzhb .NET FRAMEWORK" ["Formation Of Information Protection Competence To Students Of It-Specialties With Using .NET FRAMEWORK Cryptographic Services. "] *Physical and Mathematical Education*, 19(1), pp.48-54, 2019 (in Ukrainian).

[9] Khalimov, G. *Universal'noye kheshirovaniye*. [*Universal hashing.*] LAP LAMBERT Academic Publishing, 2014. (in Russian).

[10] K.A.Tyurin, "Nechotkoye kheshirovaniye v zadachakh informatsionnoy bezopasnosti", ["Fuzzy Hashing in Information Security Tasks"] *Overview. NCPTI*, 1(16), c. 40-53, 2019. (in Russian).

[11] N. Virt, *Algoritmy i struktury dannykh* [*Algorithms and data structures*]. M: Mir, 1989. (in Russian).

[12] P. Dzh. Sadaladzh, M. Fauler, *NoSQL: novaya metodologiya razrabotki nerelyatsionnykh baz dannykh*. [*NoSQL DISTILLED: A Brief Guide to the Emerging World of Polyglot Persistence*]. M: Williams, 2016. (in Russian).

[13] B. Shnayyer, *Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnyye teksty na yazyke Si*. [*Applied Cryptography. Protocols, Algorithms and Source Code in C*]. M.: Triumf, 2002. (in Russian).

[14] Khesh-funktsiyi - Onlayn Heneratory khesh - Convert String [Online] Available at: https://www.convertstring.com/uk/Hash [Mar. 8, 2020] (in Ukrainian).

[15] Yu.D. Zhdanova, S.O. Spasiteleva, and S.M. Shevchenko. "Zastosuvannya biblioteky klasiv Security.Cryptography dlya praktychnoyi pidhotovky spetsialistiv z kiberbezpeky" ["The Application of the Security.Cryptography Class Library for the Practical Training of Cyber Security Specialists"] *Kiberbezpeka: osvita, nauka, tekhnika*, 4(4), S.44-53, 2019. (In Ukrainian).

[16] S.O. Spasiteleva, V.L. Buriachok, "Perspektyvy rozvytku dodatkiv blokcheyn v Ukrayini" ["Perspectives For Development Of Blockchainapplications In Ukraine"], *Kiberbezpeka: osvita, nauka, tekhnika*, 1(1), c. 35-48, 2018. (in Ukrainian).